Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2014–2015

33 509 Wijziging van de Wet cliëntenrechten zorg, de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens)

C

MEMORIE VAN ANTWOORD

Ontvangen 26 maart 2015

Algemeen

Met belangstelling heb ik kennis genomen van het verslag van de vaste commissie voor Volksgezondheid, Welzijn en Sport betreffende het voorbereidend onderzoek van het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens d.d. 3 maart 2015. De gestelde vragen geven mij de gelegenheid de inhoud van dit wetsvoorstel te verduidelijken.

Bij het beantwoorden van de vragen houd ik de zoveel mogelijk de volgorde van het verslag aan. Daarbij handhaaf ik de door u gehanteerde indeling in vier onderdelen: Huidige infrastructuur en opzet wetsvoorstel, Gegevensuitwisseling en positie patiënt, Toezicht en handhaving, Reacties derden.

Inleiding

Als gegevens elektronisch worden uitgewisseld moet dat op een goede en veilige manier gebeuren. Voorwaarde daarbij is respect voor de privacy van de patiënt. Het doel van het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens, is dan ook de rechten van de cliënt te beschermen.
Het wetsvoorstel komt tegemoet aan de wensen en moties vanuit zowel uw Kamer als de Tweede Kamer. Ook is goed geluisterd naar de veldpartijen. Het wetsvoorstel regelt de randvoorwaarden waaronder veilige elektronische gegevensuitwisseling kan plaatsvinden en maakt duidelijk welke extra rechten en waarborgen voor cliënten van toepassing zijn bij elektronische gegevensuitwisseling en bij het beschikbaar stellen van gegevens via een elektronisch uitwisselingssysteem. Het is een algemeen wetsvoorstel, het heeft betrekking op cliëntenrechten bij het gebruik van alle elektronische uitwisselingssystemen. Daarbij zij nadrukkelijk opgemerkt dat van inhoudelijke of beleidsmatige bemoeienis met die systemen geen sprake is. Het wetsvoorstel en de AMvB met technische en organisatorische eisen geven slechts de voorwaarden aan, waaraan moet

kst-33509-C
ISSN 0921 - 7371
's-Gravenhage 2015

worden voldaan bij het gebruik van een elektronisch uitwisselingssysteem.
De regels die in de bestaande wetgeving zijn opgenomen met betrekking tot papieren dossiers gelden in het algemeen ook voor elektronische dossiers. Uit de juridische analyse die is uitgevoerd naar aanleiding van de motie Y van het lid Tan c.s. (Kamerstukken I 2010/11, 31 466, Y) komt naar voren dat op een aantal punten een aanpassing van de huidige wetgeving nodig is. Dit wetsvoorstel regelt deze punten: gespecificeerde toestemming voor het beschikbaar stellen en raadplegen van gegevens, het recht op elektronische inzage in en dito afschrift van gegevens, informatieplicht voor zorgaanbieders t.a.v. de rechten van cliënten bij elektronische gegevensuitwisseling. In een algemene maatregel van bestuur op grond van artikel 26 Wbp worden specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling in zijn algemeenheid geregeld. Daarnaast wordt in het wetsvoorstel uitvoering gegeven aan de motie Kuiken c.s. (Kamerstukken II, 2011/12, 27 529, nr. 99) om misbruik van elektronische uitwisselingssystemen door zorgverzekeraars te voorkomen door het stellen van een verbod op toegang en misbruik te sanctioneren.
De verantwoordelijke voor een elektronisch uitwisselingssysteem moet ervoor zorgen dat de uitwisseling veilig is en voldoet aan deze wet- en regelgeving. Dit houdt onder andere in dat de verantwoordelijke voor de gegevensverwerking ervoor moet zorgen dat de gegevens niet in verkeerde handen terecht kunnen komen.
Het College Bescherming Persoonsgegevens (CBP) houdt toezicht op de verwerking van de persoonsgegevens en de Inspectie voor de Gezondheidszorg (IGZ) op het leveren van verantwoorde zorg.

1 Huidige zorginfrastructuur en opzet wetsvoorstel

De leden van de **VVD**-fractie vragen naar de ontwikkelingen omtrent elektronische patiëntendossiers sinds de verwerping van het wetsvoorstel voor een landelijk elektronisch patiëntendossierdossier. In verband daarmee stelt men een aantal concrete vragen. Uit de vragen valt op te maken dat de leden van de VVD-fractie met «elektronische patiëntendossiers» bedoelen: elektronische uitwisselingssystemen. De vraag of de gegevensuitwisseling regionaal of landelijk gebeurt, wordt verderop in deze memorie van antwoord behandeld in samenhang met andere vragen over (regionale) gegevensuitwisseling.
Volgens informatie van Nictiz, het expertisecentrum voor standaardisatie en eHealth, vindt elektronische gegevensuitwisseling tussen zorgverleners op veel verschillende manieren plaats, waardoor het lastig is om alle systemen te achterhalen. De vraag hoeveel mensen er in een systeem voor elektronische gegevensuitwisseling zijn opgenomen is navenant lastig te beantwoorden. Het systeem met de grootste reikwijdte momenteel is het Landelijk Schakelpunt. Per 2 maart 2015 was het aantal aangemelde cliënten ruim 7 miljoen (7.177.543 unieke burgerservicenummers).
Wat betreft de instemming met en of belasting van de huisarts ten aanzien van elektronische gegevensuitwisseling het volgende. Het NIVEL, Nederlands instituut voor onderzoek van de gezondheidszorg, heeft in 2015 in opdracht van de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) de opvattingen en ervaringen van zorgverleners en zorggebruikers ten aanzien van elektronische gegevensuitwisseling inzichtelijk gemaakt. Uit dit onderzoek is naar voren gekomen dat zorgverleners en gebruikers het eens zijn over het nut van elektronische uitwisseling van medische gegevens. De bereidheid onder zorggebruikers om toestemming voor gegevensuitwisseling te geven is volgens het onderzoek groot. Uit onderzoek in april 2014 van de cliëntenfederatie NPCF komt een soortgelijk beeld naar voren. De respondenten die

aangaven geen toestemming te geven voor elektronische gegevensuitwisseling deden dat vanwege aarzelingen rond het beeld over de borging van hun privacy.
Het draagvlak onder zorgverleners, zo stelt het NIVEL rapport, wordt mede bepaald door de kwaliteit van de uit te wisselen gegevens, dekkingsgraad van cliëntendossiers en de werking van het systeem voor elektronische gegevensuitwisseling. Dit zijn aspecten die met name door de sector zelf moeten worden opgepakt. Zo werkt de sector aan de ontwikkeling en het gebruik van eenduidige standaarden om zodoende kwaliteit van de uit te wisselen gegevens te verbeteren. Ten aanzien van het opt-in systeem en de wijze waarop het geven van toestemming door de cliënt nu is geregeld, zijn de meningen van zorgverleners verdeeld; een deel van hen vindt het opt-in systeem omslachtig.

De leden van de **VVD**-fractie vernemen graag hoe het nu precies zit met de verplichting van een huisarts om mee te doen met een elektronisch uitwisselingssysteem. De leden van de fractie van de **PvdA** vragen of is uitgesloten dat zorgverzekeraars via contractering deelname aan elektronische uitwisselingssystemen afdwingen.
Uitgangspunt is dat zowel de zorgaanbieder als de cliënt zich vrij moet voelen om wel of niet deel te nemen aan een elektronisch uitwisselingssysteem. Zorgverzekeraars Nederland (ZN) heeft bevestigd eveneens geen voorstander te zijn van een financiële stimulans, laat staan verplichting, richting deelname of niet-deelname. Daarvan is dan ook geen sprake. Huisartsen en apothekers krijgen alleen een tegemoetkoming in de kosten die zij maken voor aansluiting op een elektronisch uitwisselingssysteem en het informeren van cliënten rond het vragen en verwerken van toestemming. ZN geeft aan dat zorgverzekeraars daarbij via de contractering de eis stellen dat zorgaanbieders zich aan wet- en regelgeving houden ten aanzien van het onderling delen van gegevens via een elektronisch uitwisselingssysteem. Dat betekent dat het systeem conform de eisen beveiligd moet zijn en dat om uitdrukkelijke toestemming van de cliënt wordt gevraagd om medische gegevens te mogen delen.
Mochten er signalen komen die er op duiden dat zorgaanbieders zich door financiële tegemoetkomingen toch gedwongen voelen aan te sluiten op een elektronisch uitwisselingssysteem dan zal de ik daarop actie ondernemen.
De leden van de fractie van de VVD verwijzen naar een juridische procedure rond een verzekeraar die huisartsen dwingt tot deelname aan een elektronisch cliëntendossier. Ervan uitgaande dat de VVD verwijst naar de uitspraak van de rechtbank Midden-Nederland van 23 juli 2014 in de zaak Vereniging Praktijkhoudende Huisartsen (VPH) tegen de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ, zaak nr. ECLI:NL:RBMNE:2014:3097), merk ik op dat in die zaak niet door de rechter is geoordeeld dat een verzekeraar huisartsen mag dwingen deel te nemen aan een elektronisch patiëntendossier. De omstandigheid dat de rechtbank onvoldoende aanknopingspunten ziet om te concluderen dat het belang van VZVZ – dat zo veel mogelijk cliënten worden aangesloten op de zorginfrastructuur omdat verzekeraars hun financiering afhankelijk maken van het aantal aansluitingen en de mate van gebruik van de zorginfrastructuur – heeft geleid tot het uitoefenen van ongeoorloofde druk op de individuele cliënt om zijn toestemming te geven, gaat over het belang van VZVZ en niet op individuele acties van verzekeraars tegen huisartsen.
De leden van de fractie van de **VVD** vragen zich af of dit wetsvoorstel teveel verplichtingen met zich meebrengt, of de huisarts niet overvraagd wordt en of er een financiële tegemoetkoming tegenover staat.
Het doel van het onderhavige wetsvoorstel is de bescherming van de persoonlijke levenssfeer van cliënten. Om dit te realiseren verplicht het wetsvoorstel zorgaanbieders de cliënt om toestemming te vragen voor

het beschikbaar stellen en raadplegen van gegevens, de cliënt aanvullend op de reeds bestaande informatieplicht te informeren over zijn rechten bij elektronische gegevensuitwisseling en de cliënt desgevraagd kosteloos elektronische inzage in of afschrift te geven van zijn medische gegevens. Deze verplichtingen vormen een nadere specificering op de reeds bestaande verplichtingen rond het informeren van de cliënt, het vragen van toestemming en het verschaffen van inzage in en een afschrift van het dossier van de cliënt. Zoals hierboven reeds opgemerkt ontvangen huisartsen en apothekers via de zorgverzekeraar een tegemoetkoming in de kosten die zij maken voor aansluiting op een elektronisch uitwisselingssysteem en voor het vragen en verwerken van de toestemmingsvraag aan cliënten.

De leden van de **VVD**-fractie vragen zich af wie verantwoordelijk zijn voor de uitrol en het beheer van een elektronisch uitwisselingssysteem, in hoeverre de partijen hier zelf belang bij hebben en wie de kosten bepaalt en tegen welke voorwaarden.
Het onderhavige wetsvoorstel biedt randvoorwaarden voor die situaties waarin zorgaanbieders gebruik maken van een elektronisch uitwisselingssysteem, het gebruik ervan wordt echter niet voorgeschreven of verplicht. Zoals u weet heb ik geen financiële, beleidsinhoudelijke of organisatorische betrokkenheid bij het landelijk schakelpunt of enig ander systeem voor elektronische gegevensuitwisseling. Gebruikers en beheerders van elektronische uitwisselingssystemen zijn dus zelf verantwoordelijk voor de kosten, de uitrol en het beheer ervan.

De leden van de **PvdA**-fractie geven aan in de veronderstelling te zijn dat het onderhavige wetsvoorstel tot stand is gekomen (mede) naar aanleiding van de motie-Tan c.s., ingediend en door de Eerste Kamer aangenomen in het debat over het EPD op 5 april 2011 en verbaasd te zijn dat de regering in haar reactie op het advies van de Raad van State slechts spreekt van de moties die in de Tweede Kamer zijn aangenomen.
De veronderstelling van de leden van de PvdA-fractie is terecht. Dit wetsvoorstel is in de eerste plaats tot stand gekomen naar aanleiding van de motie-Tan c.s., zoals ook expliciet wordt verwoord in de memorie van toelichting. In de memorie van toelichting worden vervolgens ook de andere moties genoemd die zijn verwerkt in dit wetsvoorstel. Bij het vragen van advies aan de Afdeling advisering van de Raad van State is vervolgens expliciet aandacht gevraagd voor de wijze waarop in het wetsvoorstel uitvoering wordt gegeven aan de motie Kuiken c.s. (Kamerstukken II, 2011/12, 27 529, nr. 99). Deze specifieke adviesvraag kwam niet voort uit het feit dat deze motie de kern van het wetsvoorstel betreft, maar werd gesteld in het licht van de uitleg die moet worden gegeven aan de Europese richtlijnen inzake het schadeverzekeringsbedrijf, en ter vervanging daarvan richtlijn 2009/138/EG (Solvency II).
Meerdere fracties (**PvdA**, **SP**) vragen welke elektronische uitwisselingssystemen er zijn. Nictiz en het NIVEL voeren jaarlijks een onderzoek uit naar de beschikbaarheid en het gebruik van eHealth toepassingen, de eHealth monitor. Elektronische gegevensuitwisseling maakt daar deel van uit. Volgens de informatie van Nictiz vindt elektronische gegevensuitwisseling tussen zorgverleners op veel verschillende manieren plaats. Een compleet overzicht van alle systemen ontbreekt. Voorbeelden van systemen waarmee gegevens in de zorg elektronisch worden uitgewisseld zijn het Landelijk Schakelpunt (LSP, een landelijk werkend systeem voor huisartsen, apothekers en medisch specialisten, gegevens worden regionaal uitgewisseld), OZIS (landelijk beschikbaar, gegevens worden regionaal uitgewisseld binnen OZIS ringen tussen apotheken, apotheekhoudende huisartsen en ziekenhuizen) en verschillende regionale netwerken op basis van de zogenaamde IHE-XDS standaard.

In vervolg op en in samenhang met de vraag naar welke systemen voor elektronische gegevensuitwisseling er zijn, is door meerdere fracties (**VVD**, **PvdA**, **D66**, **ChristenUnie**) de vraag gesteld of de elektronische gegevensuitwisseling- met het oog op motie Y van het lid Tan – beperkt blijft tot de regio of dat ook buitenregionale uitwisseling mogelijk is. Zoals gezegd bij het antwoord op de vraag naar welke systemen voor elektronische gegevensuitwisseling er zijn, werken de bekende systemen regionaal. Met dit wetsvoorstel en de AMvB op grond van artikel 26 Wbp met functionele, technische en organisatorische eisen wordt uitvoering gegeven aan de motie Tan c.s. zodat veilige uitwisseling binnen een regio mogelijk is. Er wordt geen systeem voorgeschreven. Desgewenst is bovenregionale gegevensuitwisseling mogelijk. Bij het LSP geldt dat bijvoorbeeld voor academische en gespecialiseerde ziekenhuizen die doorgaans patiënten hebben die uit meerdere regio's afkomstig zijn.
Ook vragen meerdere fracties (**VVD**, **PvdA**) of toestemming wordt gevraagd voor regionale en eventuele buitenregionale uitwisseling. Wat betreft de toestemmingvraag: voor alle systemen voor elektronische gegevensuitwisseling geldt dat ze moeten voldoen aan de bestaande wet- en regelgeving als de Wet bescherming persoonsgegevens (Wbp) en de Wet geneeskundige behandelovereenkomst (WGBO). Dat betekent ondermeer dat – los van het feit of gegevens regionaal of bovenregionaal worden uitgewisseld – altijd om toestemming van de cliënt moet worden gevraagd, zowel bij het beschikbaar stellen als bij het raadplegen van gegevens.

De leden van de fracties van de **SP** en **D66** vragen om inzicht in de cijfers van het gebruik van het LSP. Daarnaast vragen de leden van de fractie van de **SP** of de elektronische gegevensuitwisseling via het LSP regionaal verloopt.
Blijkens de cijfers die de beheerder van het LSP, de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) op haar website publiceert, is de stand van zaken per 2 maart 2015:

Aangesloten huisartsenpraktijken	3.558 (87% van het totaal aantal huisartsenpraktijken)
Aangesloten apotheken	1.822 (92% van het totaal aantal apotheken)
Aangesloten huisartsenposten	122 (99% van het totaal aantal huisartsenposten)
Aangesloten ziekenhuizen	63 (65% van het totaal aantal ziekenhuizen)
Totaal	5.565 (88% van het totaal)

Ruim 7 miljoen Nederlanders hebben toestemming gegeven aan een of meer zorgverleners om zijn of haar gegevens beschikbaar te stellen via het LSP.
De schotten tussen regio's, waarnaar de leden van de fractie van de SP verwijzen, zijn inderdaad aangebracht: de elektronische uitwisseling via het LSP verloopt regionaal. Uit de informatie van de VZVZ blijkt dat het LSP is opgedeeld in 43 regio's waarbinnen op het LSP aangesloten zorgverleners elektronisch gegevens met elkaar kunnen uitwisselen. Uiteraard mag dat alleen als er een behandelrelatie is met de patiënt én als hij daar daarvoor uitdrukkelijk toestemming heeft gegeven. Omdat de cliënten van ziekenhuizen veelal uit meerdere regio's komen, is hier een uitzondering gemaakt: academische en gespecialiseerde ziekenhuizen kunnen, als daar toestemming voor is gegeven, landelijk medicatiegegevens van hun patiënten raadplegen.

De leden van de fractie van **D66** vragen inzicht te geven in het functioneren van het Landelijk Schakelpunt (LSP).
Het is in de eerste plaats aan de toezichthouders toezicht te houden of de (elektronische) gegevensuitwisseling via het LSP (maar ook via andere elektronische uitwisselingsystemen) veilig en effectief en dus conform de geldende wet- en regelgeving verloopt. Zo heeft het College Bescherming Persoonsgegevens (CBP) recent een onderzoek afgerond naar het functioneren van het LSP (Onderzoek naar de toestemming voor de uitwisseling van medische persoonsgegevens van het LSP d.d. 1 september 2014). Behoudens enkele administratieve oneffenheden rond het verwerken van de toestemming van cliënten, constateert het CBP dat het LSP conform de Wet bescherming persoonsgegevens handelt. De VZVZ heeft – nog voor de afronding van het onderzoek – voldoende technische en organisatorische maatregelen genomen om te waarborgen dat alleen medische gegevens van mensen waarvan zeker en controleerbaar is dat ze toestemming hebben gegeven worden uitgewisseld.

De leden van de fracties van de **VVD**, **SP** en **D66** vragen zich af of het wetsvoorstel dat nu voorligt, is toegesneden op één bepaald landelijk elektronisch uitwisselingssysteem c.q. het LSP. Dat is niet het geval. In tegenstelling tot het wetsvoorstel dat betrekking had op de ontwikkeling van een landelijk elektronisch patiëntendossier dat in 2011 werd afgewezen door uw Kamer, kent het onderhavige wetsvoorstel geen verplichting voor zorgaanbieders om aan te sluiten op een (bepaald) systeem voor elektronische gegevensuitwisseling. Het wetsvoorstel is een generiek wetsvoorstel. Het bevat randvoorwaarden voor het eventuele gebruik van een elektronische uitwisselingssystemen, waar het LSP er slechts één van is. Als gebruik wordt gemaakt van een systeem dat op grond van deze wet wordt aangemerkt als een elektronisch uitwisselingssysteem, gelden daarbij de in dit wetsvoorstel neergelegd cliëntenrechten.

Het door de leden van de **CDA**-fractie genoemde lijstje (de plicht van de zorgverlener om vooraf toestemming te vragen aan de patiënt om gegevens opvraagbaar te maken ten behoeve van elektronische uitwisseling (opt-in) en deze als zodanig te gebruiken; het recht van de patiënt om (een) bepaalde (categorie van) hulpverleners op voorhand van de gegevensuitwisseling uit te sluiten; het recht van de patiënt om elektronische inzage in een dossier c.q. een afschrift daarvan te krijgen; het stellen van specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling in het algemeen), is inderdaad de kern van het wetsvoorstel. Daarnaast wordt in het wetsvoorstel uitvoering gegeven aan de motie Kuiken c.s. (Kamerstukken II, 2011/12, 27 529, nr. 99) om misbruik van elektronische uitwisselingssystemen door zorgverzekeraars te voorkomen door het stellen van een verbod op toegang en misbruik te sanctioneren.

De leden van de **SP**-fractie willen graag weten of het gesprek met het veld al concrete informatie heeft opgeleverd over de termijn waarop de elektronische uitwisselingssystemen technisch gereed zijn voor gespecificeerde toestemming.
Deze ogenschijnlijk simpele vraag blijkt in de praktijk lastig eenduidig te beantwoorden. In de afgelopen maanden zijn meerdere overleggen geweest met diverse veldpartijen. Een viertal dilemma's is naar voren gekomen.
Zo is er een grote diversiteit aan systemen in het zorgveld. Het blijkt technisch een lastige opgave de systemen gereed te krijgen voor gespecificeerde toestemming. De systemen zijn zeer divers en het ontbreekt aan onderlinge samenhang. Dat maakt dat het een lastige zoektocht is om de verschillende systemen technisch eenduidig in te

richten voor het vragen van gespecificeerde toestemming. Het is zelfs de vraag of dit voor alle systemen mogelijk zal zijn.
Daarnaast is het de vraag hoe systemen dusdanig ingericht kunnen worden dat het voor de cliënt overzichtelijk blijft aan wie en waarvoor hij toestemming heeft gegeven. Om cliënten te faciliteren in het beheren van de toestemmingen, is een centrale beheermogelijkheid gewenst dan wel noodzakelijk.
Op de derde plaats zijn voor zowel «zorgaanbieders» als «gegevens» geen eenduidige categorieën beschikbaar. Categorieën zullen vermoedelijk ook niet statisch zijn, waardoor dit leidt tot onduidelijke toestemming. Daarbij doet een categorie niet altijd recht aan de belevingswereld; een labuitslag over waardes van bloedglucose heeft voor een cliënt een andere lading dan de labuitslag voor HIV.
Tenslotte: naast de aanpassing van systemen voor de registratie van toestemming zullen informatiesystemen ook moeten acteren op basis van vastgelegde toestemming; bijvoorbeeld het versturen van een overdrachtsdocument zonder de labgegevens indien deze door de cliënt zijn uitgesloten.
Partijen hebben dit vraagstuk inmiddels, gecoördineerd door Nictiz, opgepakt vanuit het cliëntperspectief met als doel te komen tot een werkbare systematiek voor zorgaanbieder en cliënt. Via het Informatieberaad, het zorgbreed bestuurlijk overleg met partijen uit het veld, wordt de brede betrokkenheid van veldpartijen bij onder andere dit vraagstuk gewaarborgd.
Het benoemen van een exact moment waarop systemen technisch gereed zullen zijn, is op dit moment nog niet haalbaar. Na de behandeling van het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens in uw Kamer wordt een ingangsdatum voor inwerkingtreding van de wet bepaald, inclusief een overgangstermijn. Dit zal uiteraard een realistische termijn moeten zijn. Desondanks is het cruciaal dat het onderhavige wetsvoorstel tot wet wordt verheven. Vanuit cliëntenperspectief is het belangrijk om scherp te stellen waar de elektronische gegevensuitwisseling aan moet voldoen. Dat geeft helderheid aan het veld en benadrukt de urgentie voor de cliënt.

De leden van de fractie van de **SP** vragen of de Inspectie voor de Gezondheidszorg (IGZ) haar onderzoek naar het functioneren van de elektronische uitwisselingssystemen heeft herhaald.
De IGZ heeft door middel van een quick scan naar het gebruik van standaarden van elektronische informatie-uitwisseling in de zorg, geïnventariseerd hoe ver het veld inmiddels is gevorderd met de aanbevelingen uit het onderzoek waarnaar de leden van de SP-fractie verwijzen, de Staat van de Gezondheidszorg 2011. Deze quick scan heb ik op 28 oktober jongstleden aangeboden aan de leden van de Tweede Kamer.
De IGZ concludeert op basis van de quick scan dat er stappen zijn gezet op het gebied van standaardisatie van informatie-uitwisseling. Toch worden standaarden nog niet door alle zorgaanbieders geïmplementeerd. Om de ontwikkeling en het gebruik van standaarden in de zorg verder te bevorderen, zijn in navolging van dit advies diverse acties uitgezet.
Het Zorginstituut Nederland richt zich op de verbetering van de kwaliteit van de gezondheidszorg en meet dit aan de hand van vorderingen in het toepassen van kwaliteits- en informatiestandaarden.
Daarnaast zijn er veel initiatieven vanuit de sector zelf op het gebied van ontwikkeling en gebruik van standaarden met als doel het verbeteren van de kwaliteit van de informatie en dus de zorg, die samen komen in het Informatieberaad. Hier werken zorgaanbieders, zorgverzekeraars, koepels en de overheid samen bij het kiezen voor duurzame oplossingen voor de informatie-uitwisseling en de implementatie. Door middel van het Informatieberaad wordt commitment van de betrokken partijen gereali-

seerd omdat we gezamenlijk, als overheid en sector daar een belangrijke verantwoordelijkheid bij hebben.
Op deze manier wordt gebruik en implementatie van standaarden mede geborgd.

De leden van de fractie van **D66** nodigen de regering uit een toelichting te geven over de toegevoegde waarde van het wetsvoorstel naast de bestaande regelgeving in Wbp, Wet BIG en WGBO.
Naar aanleiding van de motie van het lid Tan c.s. is een juridische analyse uitgevoerd (Kamer-stukken II, 2010/2011, 27 529, nr. 82) waarbij is bekeken in hoeverre bestaande wetten dienen te worden aangepast met het oog op veilige en betrouwbare elektronische gegevensuitwisseling in de zorg. Uit deze analyse komt naar voren dat op een aantal punten een aanpassing van de huidige wetgeving dient plaats te vinden.
De regels die in de bestaande wetgeving zijn opgenomen met betrekking tot dossiers in het algemeen gelden ook voor elektronische dossiers. Het wetsvoorstel introduceert een aantal normen dat specifiek betrekking heeft op elektronische verwerking van gegevens in de zorg. Enerzijds gaat het om de uitdrukkelijke en gespecificeerde toestemming om gebruik te kunnen maken van een elektronisch uitwisselingssysteem, anderzijds zijn de rechten vastgelegd rond elektronische inzage en afschrift en nadere bepalingen rond de logging van gegevens. De in dit wetsvoorstel opgenomen bepalingen zien op deze specifieke vorm van verwerking van gegevens in de zorg en zijn om die reden bij elkaar in een apart wetsvoorstel geplaatst.
Het doel van het wetsvoorstel is het verbeteren van de kwaliteit van de zorg en het verbeteren van de patiëntveiligheid door duidelijk te maken welke extra rechten en waarborgen voor cliënten van toepassing zijn bij elektronische gegevensuitwisseling en de beschikbaarheid van gegevens via een elektronisch uitwisselingssysteem.

2 Gegevensuitwisseling en positie patiënt

De leden van de fractie van de **VVD** vragen in hoeverre de Minister verantwoordelijk is voor het reilen en zeilen van elektronische uitwisselingssystemen en welke mogelijkheden zij heeft om in te grijpen als zaken niet conform de regels verlopen.
De verantwoordelijkheid van de Minister richt zich op het creëren van randvoorwaarden waaronder veilige elektronische gegevensuitwisseling kan plaatsvinden. In het nu voorliggende wetsvoorstel zijn de rechten voor cliënten opgenomen die gelden bij elektronische uitwisseling van zijn gegevens tussen zorgaanbieders. In een algemene maatregel van bestuur worden alle technische eisen opgenomen waaraan elektronische uitwisselingssystemen en zorginformatiesystemen moeten voldoen. Daarnaast gelden de wettelijke eisen van de Wbp en de Wet op de geneeskundige behandelingsovereenkomst (WGBO). De verantwoordelijke voor een elektronisch uitwisselingssysteem moet ervoor zorgen dat de uitwisseling veilig is en voldoet aan deze wet- en regelgeving. Dit houdt onder andere in dat de verantwoordelijke voor de gegevensverwerking ervoor moet zorgen dat de gegevens niet in verkeerde handen terecht kunnen komen.
Het College Bescherming Persoonsgegevens (CBP) houdt toezicht op de verwerking van de persoonsgegevens en de Inspectie voor de Gezondheidszorg (IGZ) op het leveren van verantwoorde zorg. Mochten de toezichthouders daartoe aanleiding zien dan kunnen zij handhavend optreden.
Volgens de leden van de **PvdA**-fractie kiest het wetsvoorstel nogal eens de positie van de zorgaanbieder als uitgangspunt.
Het doel van het wetsvoorstel is om de patiëntveiligheid te verbeteren door extra rechten en waarborgen voor cliënten uiteen te zetten die van

toepassing zijn bij elektronische gegevensuitwisseling en de beschikbaarheid van gegevens via een elektronisch uitwisselingssysteem. Voordat een zorgaanbieder gegevens van de cliënt beschikbaar stelt via een elektronisch uitwisselingssysteem, dient hij bijvoorbeeld vast te stellen dat de cliënt daarvoor uitdrukkelijk toestemming heeft gegeven. De cliënt heeft bovendien recht op kosteloze elektronische inzage in of afschrift van de gegevens in zijn dossier of de gegevens die via een elektronisch uitwisselingssysteem beschikbaar zijn gesteld. Op verzoek van de cliënt wordt tevens opgenomen wie bepaalde informatie beschikbaar heeft gesteld dan wel heeft ingezien of opgevraagd en op welke datum.
Om deze rechten en waarborgen voor cliënten te bewerkstelligen is het noodzakelijk dat zorgaanbieders in lijn met deze rechten en waarborgen handelen. De kwaliteit, de correctheid, de volledigheid en het up to date zijn van het medisch dossier, valt onder de verantwoordelijkheid van de zorgaanbieder. Om die reden heeft een aantal van de artikelen in het wetsvoorstel betrekking op het handelen van de zorgaanbieder. De rechten en waarborgen van cliënten zijn echter steeds het uitgangspunt.

In vervolg hierop stellen de leden van de **PvdA**-fractie een aantal vragen over de wijze waarop een cliënt overzicht krijgt van wie zijn gegevens bewaart, over hoe lang de gegevens bewaard worden en over de overdracht van zijn gegevens naar een nieuwe huisarts. Dit verschilt niet met de huidige situatie.
Met dit wetsvoorstel wordt nadrukkelijk geen bepaald, centraal elektronisch uitwisselingssysteem voorgeschreven en er is ook geen sprake van centrale opslag van data. Dat betekent dat het antwoord op deze vraag afhankelijk is van het aantal zorgaanbieders waar de cliënt onder behandeling is geweest en de inrichting van hun informatiesystemen. Een zorgaanbieder mag alleen informatie uit het door hem bijgehouden medisch dossier verstrekken. Dit betekent in beginsel dat de cliënt, net als in de huidige situatie, alle zorgaanbieders bij wie hij onder behandeling is geweest afzonderlijk langs moet gaan om een compleet overzicht te krijgen. Soms zal er sprake van zijn dat opvolgende zorgaanbieders in dezelfde beroepsgroep (bijvoorbeeld huisartsen) het medisch dossier van de cliënt overdragen. Dit betreft overdracht met toestemming van de cliënt omdat hij overstapt naar die andere huisarts. Dit geldt zowel voor papieren als elektronische dossiers. De toegang van de «oude» huisarts tot het medisch dossier wordt dan beëindigd.
In de wet is als hoofdregel neergelegd (artikel 7:454, derde lid BW) dat een medisch dossier minimaal 15 jaar moet worden bewaard na het einde van de behandelingsovereenkomst. Wanneer een nieuwe zorgaanbieder het medisch dossier overneemt, neemt hij ook de dossierplicht en de bewaartermijn over van zijn voorganger.

De leden van de **PvdA**-fractie stellen terecht dat de zorgverzekeraar geen toegang heeft tot elektronische uitwisselingsystemen. Zij vragen zich af hoe zich dit verhoudt tot andere mogelijkheden voor zorgverzekeraars om kennis te nemen van de inhoud van patiëntendossiers (waaronder diagnosestellingen).
Als een zorgverzekeraar voor het uitvoeren van zijn wettelijke controles gegevens nodig heeft uit het patiëntendossier dat wordt bijgehouden door een zorgaanbieder, dan is de zorgaanbieder verplicht die gegevens te verstrekken aan de zorgverzekeraar. De zorgverzekeraar hoeft daarvoor zelf geen toegang te hebben tot het patiëntendossier.
Zorgverzekeraars hebben alleen de mogelijkheid om kennis te nemen van de inhoud van patiëntendossiers (waaronder diagnosestellingen) als dat noodzakelijk is voor het uitvoeren van een zogenoemde materiële controle. Bij materiële controle controleert de zorgverzekeraar of een zorgverlener een gedeclareerde prestatie daadwerkelijk heeft geleverd en

of die prestatie het meest was aangewezen gezien de gezondheidstoestand van de verzekerde.
Het opvragen van medische informatie – als detailcontrole – is alleen toegestaan als er na algemene controlestappen bij de verzekeraar onvoldoende vertrouwen bestaat dat de declaratie aan de gestelde eisen voldoet. Als de controle door middel van een minder belastend instrument mogelijk is, dan moet deze eerst worden toegepast. Inzage in patiëntendossiers door zorgverzekeraars mag daarom alleen plaatsvinden als uiterste middel.
Er geldt een strikte procedure voor het opvragen van medische informatie bij de zorgverlener door de zorgverzekeraar als deze een materiële controle uitvoert. Deze procedure is voorgeschreven in de Zorgverzekeringswet en de daarop gebaseerde Regeling Zorgverzekering. De in de regels omschreven procedure is uitgewerkt in het op die regeling gebaseerde Protocol materiële controle, dat onderdeel uitmaakt van de Gedragscode verwerking persoonsgegevens zorgverzekeraars van ZN. Voldoet de verzekeraar aan de in de Zorgverzekeringswet (Zvw) en de Regeling gestelde eisen, dan is de zorgaanbieder verplicht zijn medewerking te verlenen aan de controle.

De leden van de fractie van het **CDA** vragen naar de procedure van logging en willen weten of een overzicht van de logging bij elektronische gegevensuitwisseling kosteloos wordt verstrekt.
Het bijhouden van loggegevens is verplicht op grond van art. 35, tweede lid van de Wbp. In het onderhavige wetsvoorstel is daaraan in art. 15e Wbsn-z toegevoegd dat de cliënt die een afschrift vraagt van zijn gegevens daarin kan zien wie bepaalde informatie beschikbaar heeft gesteld en op welk moment, en wie bepaalde informatie heeft ingezien of opgevraagd op welk moment. De elektronische inzage in of de verstrekking van een elektronisch overzicht van de loggegevens is kosteloos.
Als een afschrift wordt gevraagd aan zorgaanbieder A, kan de cliënt op basis van de logging zien dat zorgaanbieder B bepaalde gegevens afkomstig uit het dossier van zorgaanbieder A heeft ingezien. Zorgaanbieder A kan echter niet de gegevens die zorgaanbieder B beschikbaar heeft gesteld, aan de cliënt overleggen. Dit volgt uit de formulering van artikel 15d, eerste lid Wbsn-z: de cliënt verzoekt om een afschrift van de gegevens «betreffende deze cliënt die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt».
Via bijvoorbeeld de website van Nederlandse Patiënten en Consumenten Federatie (NPCF) zijn voorbeeldbrieven te vinden die cliënten kunnen gebruiken in hun correspondentie met hun zorgaanbieder over bijvoorbeeld logging.

In de AMvB op grond van artikel 26 Wbp worden specifieke functionele, technische en organisatorische eisen gesteld aan elektronische gegevensuitwisseling. In deze AMvB wordt voor de informatiebeveiliging in de zorg dwingend verwezen naar beschikbare normen van het Nederlands Normalisatie-instituut, te weten NEN 7510;2011 (NEN 7510) en de verdere uitwerking van deze algemene norm betreffende informatiebeveiliging in de zorg in NEN 7512 en NEN 7513.
De leden van de fractie van het **CDA** vragen of met deze dwingende verwijzing de eisen voor identificatie en authenticatie voldoende zijn afgedekt en hoe de naleving van deze normen wordt gecontroleerd.
Als een zorgaanbieder de in NEN 7510 en overige genoemde normen aangegeven maatregelen heeft getroffen, mag er inderdaad vanuit worden gegaan dat deze «passende technische en organisatorische maatregelen» heeft getroffen, als bedoeld in artikel 13 van de Wet Bescherming Persoonsgegevens (Wbp). De verplichting om aan de normen in het besluit te voldoen rust in de eerste plaats op de verant-

woordelijke in de zin van de Wbp. Dit is de partij die het elektronisch uitwisselingssysteem in stand houdt en het doel en de middelen van de gegevensverwerking bepaalt. Een aantal verplichtingen rust eveneens op de zorgaanbieder die is aangesloten op een elektronisch uitwisselingssysteem.
Op grond van de Wbp is het College Bescherming persoonsgegevens (CBP) de toezichthouder voor de AMvB. In haar onderzoeksrapport «Toegang tot digitale patiëntendossiers binnen zorginstellingen» (Den Haag, juni 2013, blz. 20) merkt het CBP op bij de toetsing van beveiligingsmaatregelen van zorginstellingen aan artikel 13 Wbp gebruik te maken van NEN 7510 «als ijkpunt».
Verder heeft de IGZ op grond van de Kwaliteitswet zorginstellingen tot taak toezicht te houden op verantwoorde zorg. Zij zal die onderdelen van NEN 7510 die hiervoor relevant zijn in haar toezicht betrekken. De IGZ en het CBP hebben een samenwerkingsprotocol waarin de afspraken tussen hen over de wijze van samenwerking bij het toezicht is opgesteld. Mijn taak is het stellen van randvoorwaarden voor veilige elektronische gegevensuitwisseling. De technische en organisatorische eisen die in de AMvB worden gesteld, geven daarbij een duidelijk kader. Het is aan het IGZ en het CBP om de manier van toezicht houden nader in te vullen.
Heeft – zo vragen de leden van de **CDA**-fractie – de landelijke zorginfrastructuur c.q. het Landelijk Schakelpunt (LSP) eigen rechtspersoonlijkheid? Kan deze instantie zich beroepen op de beperking van de aansprakelijkheid als bedoeld bij artikel 6:196c BW?
De landelijke infrastructuur (c.q. het landelijk schakelpunt; LSP) bezit geen eigen rechtspersoonlijkheid. De Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) is beheerder van het LSP. De VZVZ is gelet op die taak – samen met de zorgaanbieders – verantwoordelijke als bedoeld in de Wet bescherming persoonsgegevens (Wbp). In het LSP worden geen medische dossiers opgeslagen en VZVZ is dus niet verantwoordelijk voor de inhoud van de gegevens die uitgewisseld worden.
De civielrechtelijke aansprakelijkheid van de beheerder van een elektronisch uitwisselingssysteem, hangt af van de overeenkomsten die hij sluit met zorgserviceproviders en zorgaanbieders en de daarin opgenomen clausules om aansprakelijkheid uit te sluiten. De verantwoordelijke zou kunnen worden aangesproken op gezondheidsschade die ontstaat doordat het elektronisch uitwisselingssysteem niet of niet naar behoren werkt. Van privacyschade kan sprake zijn als via het elektronisch uitwisselingssysteem bijvoorbeeld ten onrechte gegevens beschikbaar worden gesteld aan zorgaanbieders die door de cliënt zijn uitgesloten. In zo'n geval kan de cliënt – bijvoorbeeld op grond van artikel 49 van de Wbp – de verantwoordelijke van het elektronisch uitwisselingssysteem rechtstreeks aansprakelijk stellen. Bij gezondheidsschade door het foutief beschikbaar stellen van informatie aan een zorgaanbieder met als gevolg dood of letsel, kan de verantwoordelijke van het elektronisch uitwisselingssysteem ook strafrechtelijk aansprakelijk zijn.
Wanneer de vraag van de CDA-fractie moet worden opgevat of de VZVZ (of een andere beheerder van een elektronisch uitwisselingssysteem) zich zou kunnen beroepen op artikel 6:196c BW dan luidt het antwoord dat deze vraag enkel beantwoord kan worden aan de hand van de specifieke omstandigheden van een concreet geval.

De leden van de **CDA**-fractie vragen welke specifieke eisen worden gesteld om te bewerkstelligen dat ook bij grensoverschrijdende gegevensuitwisseling aan de in de Wbp gestelde eisen wordt voldaan. Ook vragen zij te bevestigen of het juist is dat de Patriot Act van toepassing is en of deze situatie verandert als de Verordening algemeen kader bescherming persoonsgegevens van kracht wordt.
Ook bij grensoverschrijdende gegevensoverdracht is de Wet bescherming persoonsgegevens van toepassing. Binnen EU-landen zal een gelijk-

waardig niveau van gegevensbescherming gelden ingevolge de Europese privacyregelgeving (richtlijn 95/46/EG en de concept privacyverordening). Buiten de EU kan op grond van artikel 76 Wbp alleen gegevensverwerking plaatsvinden als daar een passend beschermingsniveau geldt, dat tenminste zal moeten voldoen aan de vereisten als vervat in NEN 7510 en de uitwerking daarvan in NEN 7512 en NEN 7513.
Als wordt samengewerkt met bedrijven die gevestigd zijn in een ander land kunnen mogelijk andere rechtsregels gelden, de Patriot Act is daarvan een bekend voorbeeld. Als men voor het opzetten of beheren van een elektronisch uitwisselingssysteem in zee gaat met een bedrijf met een basis in de Verenigde Staten, zal men zich hier bewust van moeten zijn en moeten afwegen of daarover goede afspraken vastgelegd kunnen worden. In Europees verband wordt gewerkt aan bouwstenen en overeenkomsten om elektronische gegevensuitwisseling tussen lidstaten te faciliteren. In Brussel wordt onderhandeld over de door de leden van de CDA-fractie genoemde Algemene verordening gegevensbescherming. Deze verordening zal een nieuw kader bevatten voor grensoverschrijdende doorgifte van persoonsgegevens. Daarbij wordt ook aandacht geschonken aan doorgifte op grond van eenzijdige verplichtingen op grond van buitenlands recht van derde staten. De Europese Commissie gaat ervan uit dat een redelijk evenwicht is te bieden tussen de dilemma's waarin bedrijven zich soms kunnen bevinden en de bescherming van persoonsgegevens. De Minister van Veiligheid en Justitie is hierbij betrokken.

De leden van de **PVV**-fractie stellen dat er enorme risico's zouden zijn aangaande de privacy van gegevens in verband met de mogelijkheid tot hacken.
Deze wet richt zich nu juist op een betere bescherming bij elektronische gegevensuitwisseling. De Wet bescherming persoonsgegevens (Wbp) schrijft voor dat zorgverleners medische dossiers goed beveiligen. Zij moeten er bijvoorbeeld voor zorgen dat alleen bevoegde personen toegang hebben tot het dossier van een cliënt. Aanvullend wordt in de AMvB bij het onderhavige wetsvoorstel dwingend verwezen naar NEN 7510. Volgens deze norm moet een risicoanalyse worden opgesteld. Een onderdeel daarvan is het bepalen van relevante dreigingen. Onder deze dreigingen vallen opzettelijke menselijke incidenten, zoals diefstal van gegevens of kwaadaardige programmatuur. Om de risico's te kunnen beoordelen moet duidelijk zijn wat de kwaliteit is van de bestaande beveiligingsmaatregelen. Om eventuele kwetsbaarheden te kunnen ontdekken ligt het voor de hand een hack-test of penetratietest uit te voeren.
Wat betreft de vraag of de regering kan garanderen dat de gegevens in veilige handen zijn, zij opgemerkt dat het aan de zorgaanbieder is om de beveiliging op orde te hebben; de regering stelt de randvoorwaarden waaraan gebruikers van elektronische systemen voor gegevensuitwisseling tussen zorgaanbieders moeten voldoen. Als gegevens niet in veilige handen blijken te zijn kunnen eventuele gedupeerden aangifte doen van computervredebreuk (in het geval van bijvoorbeeld een hack) of aangifte van schending van de geheimhoudingsplicht.
Ook stellen de leden van de PVV-fractie dat het, in het kader van de overdracht van zorgtaken aan de gemeenten, aan eenduidige richtlijnen ontbreekt nu gemeenten afspraken hebben gemaakt met meer dan honderd softwareleveranciers die allemaal hun eigen beveiliging kennen. Zoals aangegeven stelt dit onderhavige wetsvoorstel randvoorwaarden voor elektronische gegevensuitwisseling tussen zorgaanbieders. Deze vraag heeft betrekking op elektronische gegevensuitwisseling met derden (de gemeenten). In dat geval geldt dat ook gemeenten, wijkteam, bureau Jeugdzorg, de wijkagent enzovoort moeten handelen conform de Wet bescherming persoonsgegevens. In de Wet bescherming persoonsgegevens (Wbp; artikelen 13 en 16) staat dat, rekening houdend met de

stand van de techniek en de kosten van de tenuitvoerlegging, passende technische en organisatorische maatregelen moeten worden genomen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking en dat de verwerking van persoonsgegevens betreffende iemands gezondheid in principe is verboden. Verder zijn krachtens de Jeugdwet ook beveiligingseisen gesteld door de verplichting te voldoen naar de voor beveiliging relevante NEN-normen.
De regering is het met de leden van de PVV-fractie eens dat controle op persoonsgegevens moet worden nageleefd en misbruik gestraft dient te worden. Degenen die in strijd handelen met de Wet bescherming persoonsgegevens (Wbp) kunnen op verschillende manieren worden aangesproken, zowel op grond van het privaatrecht, het bestuursrecht of het strafrecht. Ook betrokkenen die vermoeden dat er misbruik is gemaakt van hun gegevens kunnen via deze wegen hun recht halen.
Het College bescherming persoonsgegevens (CBP) ziet toe op de naleving van de Wbp. Op dit moment kan het CBP bij overtredingen van de Wbp bestuursdwang toepassen of een last onder dwangsom opleggen. In het wetsvoorstel gebruik camerabeelden en meldplicht datalekken van de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties wordt voorzien in een brede meldplicht voor datalekken, waaronder datalekken in medische systemen. Dit is vooruitlopend op de meldplicht zoals voorgesteld in de Europese privacyverordening. De bevoegde toezichthouder zal daarbij het CBP zijn.
Of extra training nodig is voor personeel dat met persoonsgegevens omgaat, zoals de leden van de PVV-fractie stellen, is niet aan de regering te beoordelen. Met het overdragen van taken naar de gemeenten is niet veranderd dat het personeel moet handelen conform de bepalingen uit de Wbp. De gemeente is zelf verantwoordelijk voor de uitvoering van de wet- en regelgeving die van toepassing is voor het omgaan met (persoons)gegevens in de gemeente. Hieronder valt ook het kweken van bewustzijn bij de medewerkers.

De leden van de **SP**-fractie vragen naar een overzicht van de onderliggende AMvB's.
Ter uitvoering van de motie Tan c.s. is een AMvB voorbereid met technische en organisatorische eisen voor elektronische uitwisselingssystemen. De grondslag voor deze AMvB[1] is te vinden in artikel 26 Wbp. Ook de leden van de **D66**-fractie vragen naar deze AMvB om deze bij de beoordeling van het wetsvoorstel te kunnen betrekken.
Deze AMvB met technische en organisatorische eisen is ter advisering voorgelegd aan de Afdeling advisering van de Raad van State. Gelet op artikel 26 van de Wet op de Raad van State, vindt openbaarmaking plaats gelijk met de bekendmaking van het besluit als het tezamen met dit wetsvoorstel in werking zal treden. U ontvangt daarom het ambtelijk concept voor deze AMvB.
Naast deze AMvB met technische en organisatorische eisen is op 19 juli 2014 een AMvB in werking getreden (Staatsblad 2014, 282) houdende wijziging van het Besluit gebruik burgerservicenummer in de zorg in verband met de aanwijzing van verantwoordelijken voor elektronische gegevensuitwisseling als zorgaanbieder. Deze wijziging van het Besluit gebruik burgerservicenummer vormt voor beheerders van elektronische uitwisselingssystemen de wettelijke grondslag om binnen de gegeven randvoorwaarden het bsn te verwerken. Dit is van belang om een hoge betrouwbaarheid van elektronische uitwisselingssystemen te kunnen waarborgen.

[1] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 156818.05.

In antwoord op de vraag van de leden van de **SP**-fractie of het Landelijk Schakelpunt (LSP) met generiek of specifieke toestemming werkt het volgende.
De beheerder van het LSP, de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) heeft hierover een heldere uitleg geplaatst op haar website. De VZVZ stelt daarin het volgende, ik citeer: «De toestemming die VZVZ en zorgaanbieders nodig hebben voor gegevensverwerking via het LSP betreft uitdrukkelijke toestemming overeenkomstig de geldende wetgeving (Wbp en WGBO). Conform die wetgeving betreft dit een gerichte, specifieke toestemming».
Ook stelt de VZVZ dat als er een aanpassing in de gegevensverwerking via het LSP zou worden voorgenomen waarbij andere soorten gegevens, andere doeleinden of andere ontvangers van de gegevens aan de orde zouden komen, dat daarvoor dan nieuwe toestemming noodzakelijk is.
Op de vraag tot welke gradatie specifieke toestemming kan gaan, wordt nader ingegaan bij het onderdeel «Reacties derden».

De leden van de fractie van de **SP** vragen naar het vervolg op de gewijzigde motie van de leden Bruins Slot en Bouwmeester van de Tweede Kamer (33 509, nr. 36) waarmee de regering wordt verzocht te bevorderen dat zorgpartijen de gedragscode EGiZ voorleggen aan het College Bescherming Persoonsgegevens en de Kamer hierover te informeren.
In een brief van 1 augustus 2014 heb ik de beheerders van de EGiZ nadrukkelijk gevraagd om de gedragscode alsnog voor te leggen aan het College Bescherming Persoonsgegevens.
In een schriftelijke reactie d.d. 3 oktober 2014 heeft de Koninklijke Nederlandse Maatschappij der Geneeskunst (KNMG) laten weten dit vooralsnog niet te zullen doen. De KNMG stelt dat als men al besluit het CBP te verzoeken om een verklaring van overeenstemming af te geven over de EGiZ, men daarmee in ieder geval mee wacht tot na de inwerkingtreding van het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens.

De leden van de fractie van **D66** vragen of de regering inzicht kan geven in het functioneren van een EPD in de ons omringende landen, of Nederland hierbij achter loopt en of in de naburige landen ervaring is opgedaan met veiligheidsrisico's.
Op verzoek van de Tweede Kamer heeft onderzoeksbureau KPMG in opdracht van het Ministerie van VWS in 2011 een quick scan uitgevoerd naar EPD-initiatieven in zes Europese landen. De resultaten daarvan zijn op 7 februari 2012 aan uw Kamer aangeboden (Internationaal onderzoek EPD's, Rapportage aan het Ministerie van VWS, 6 februari 2012).
Net als destijds in Nederland, werd in alle onderzochte landen (België, Denemarken, Duitsland, Frankrijk, Spanje en Engeland) de aanpak gericht op het realiseren van een landelijk gedeelde infrastructuur. Uit het onderzoek bleek dat de implementatie en uitrol meestal plaatsvindt vanuit een regiomodel waarbij moet worden opgemerkt wordt dat regio's hierbij een grootte van veelal enkele miljoenen inwoners hebben. De internationale EPD-programma's werden zonder uitzondering onder regie van één centrale overheidsinstantie uitgevoerd en overal is een groot aantal partijen betrokken.
Op verzoek van uw Kamer is de ontwikkeling onder regie van de overheid in Nederland te komen tot één landelijke infrastructuur waarop alle zorgaanbieders verplicht aansluiten stopgezet. Daarmee is een vergelijking c.q. een oordeel of Nederland voor of juist achter loopt, lastig te geven.
In alle landen spelen of speelden discussies op het gebied van privacy en beveiliging. Uit het KMPG-rapport blijkt dat in vier landen voor het gebruik van een landelijke EPD een opt-in aanpak gehanteerd, in twee landen

(Engeland en Spanje) koos men voor een opt-out aanpak. Toegang tot medische informatie is in alle landen door middel van de wet- en regelgeving gelimiteerd tot (een beperkte doelgroep van) zorgverleners. Afhankelijk van het land heeft de cliënt de mogelijkheid dit in detail of op globaal niveau aan te geven. Zorgverzekeraars hebben geen toegang tot medische informatie, alhoewel zij in de meeste landen niet expliciet worden uitgesloten door wetgeving. Uitzondering hierop is Frankrijk, waarin expliciet wordt aangegeven dat informatie in het dossier niet mag worden gebruikt bij het afsluiten van een zorgverzekering.

In antwoord op de vraag van de leden van de fractie van de **ChristenUnie** naar de eindverantwoordelijkheid voor de veiligheid van de uitwisseling van patiëntgegevens en de aansprakelijkheid in dit verband het volgende.
Bij het gebruik van een elektronisch uitwisselingssysteem blijven de aansprakelijkheidsrisico's grotendeels gelijk aan de aansprakelijkheidsrisico's in de situatie dat geen gegevensuitwisseling plaatsvindt. Als er iets mis gaat zal in de meeste gevallen de zorgaanbieder als eerste worden aangesproken.

De leden van de fractie van de **ChristenUnie** vragen voorts hoe wordt voorkomen dat er een oneigenlijk onderscheid wordt gemaakt tussen patiënten die wel en patiënten die geen toestemming verlenen voor het elektronisch verwerken van hun gegevens? Hoe wordt voorkomen dat het moeilijk wordt voor patiënten om geen toestemming te geven voor uitwisseling van gegevens, bijvoorbeeld omdat de kwaliteit van de dienstverleningen of zelfs van de zorg daardoor afneemt?
De eisen die worden gesteld aan de kwaliteit van de dienstverlening door zorgaanbieders, zijn vastgelegd in de Wet op de Beroepen in de Individuele Gezondheidszorg (BIG), de Kwaliteitswet zorginstellingen en voor de behandelrelatie van de cliënt en de zorgverlener gelden de eisen van de WGBO. Op grond van deze algemeen geldende eisen kan geen onderscheid gemaakt worden tussen patiënten die wel of niet hun gegevens beschikbaar laten stellen via een elektronisch uitwisselingssysteem.

De leden van de fractie van de **ChristenUnie** vragen of het niet verlenen van toestemming aan een bepaalde zorgaanbieder eenmalig is of dat er een bepaalde termijn geldt. Ook vraagt men zich af hoe een en ander praktisch en werkbaar blijft.
Cliënten hebben te allen tijde het recht om hun toestemming in te trekken dan wel aan te passen door uitbreiding of inperking. Dit impliceert dat er geen sprake is van een eenmalige uitsluitingsoptie of een bepaalde termijn. Dit wetsvoorstel schrijft geen specifiek systeem voor; de technische invulling is derhalve aan de beheerders van systemen en de zorgaanbieders zelf.
De leden van de fractie van de **ChristenUnie** geven aan dat de Nederlandse Vereniging van Ziekenhuizen (NVZ) stelt dat de voorgestelde systematiek van logging niet uit te voeren is.
Op grond van artikel 35 lid 2 van de Wbp heeft een cliënt al het recht om een overzicht op te vragen van wie zijn gegevens hebben ingezien. Zorgaanbieders zijn derhalve reeds wettelijk verplicht om bij te houden wie het dossier heeft ingezien. Artikel 15e van dit wetsvoorstel is een extra verduidelijking van artikel 35 Wpb voor wat betreft de elektronische gegevensuitwisseling; namelijk dat op verzoek van de cliënt in het afschrift (waar de cliënt om vraagt) wordt opgenomen wie bepaalde informatie via het elektronische uitwisselingssysteem beschikbaar heeft gesteld en op welke datum en wie bepaalde informatie heeft ingezien of opgevraagd en op welke datum.

De regering is er dan ook niet van overtuigd dat de voorgesteld systematiek van «logging» onmogelijk uit te voeren is. Als bedoeld wordt dat logging van alle acties in het systeem technisch niet mogelijk is en/of leidt tot risico's voor de werking van het systeem, wordt opgemerkt dat de «huidige stand van de techniek» maatgevend is voor hetgeen als passende maatregelen in de zin van artikel 13 Wbp wordt beschouwd. Het is aan de zorginstellingen om stappen te zetten om te komen tot een update/upgrade van het door hen gebruikte (verouderde) systeem. Uitgangspunt is dat een elektronisch uitwisselingssysteem moet voldoen aan de bij AMvB vast te technische en organisatorische eisen. Daarbij wordt dwingend verwezen naar NEN-normen waaronder NEN 7513 die betrekking heeft op logging. De NEN-normen komen tot stand op basis van afspraken die veldpartijen vrijwillig met elkaar maken over de kwaliteit en veiligheid van hun producten, diensten en processen, zo ook NEN 7513.

3 Toezicht en handhaving

De leden van de fractie van het **CDA** vragen een verduidelijking op de bevoegdheden, samenwerking en capaciteit van de toezichthouders: de Inspectie voor de Gezondheidszorg (IGZ) en het College Bescherming Persoonsgegevens (CBP).
Het CBP ziet toe op de naleving van de Wet bescherming persoonsgegevens en aanverwante wetten. De IGZ ziet erop toe dat er verantwoorde zorg wordt geleverd. Daar hoort ook bij dat informatie-uitwisseling in de zorg op verantwoorde wijze plaats vindt, dat wil zeggen niet meer en minder dan nodig is en dat gegevens betrouwbaar en beschikbaar zijn. Overigens maakt het daarbij niet uit of er sprake is van een mondelinge, papieren of elektronische informatie-uitwisseling is.
Meer specifiek ziet de IGZ toe op informatiebeveiliging in de zorg op basis van de bestaande norm NEN 7510 vanuit oogpunt van patiëntveiligheid. In 2015 zal de IGZ specifieke aandacht schenken aan het thema ICT in de Zorg, waarbij ook aspecten van de NEN7510 meegenomen zullen worden. Of het CBP in een specifieke situatie capaciteit inzet voor het toezicht op het elektronisch uitwisselen van medische gegevens, bepaalt het CBP aan de hand van prioriteringscriteria. De prioriteringscriteria zijn erop gericht om de capaciteit van het CBP zo efficiënt en effectief mogelijk in te zetten. In de Beleidsregels handhaving door het CBP heeft het CBP deze prioriteringscriteria vastgesteld en heeft het keuzes in het toezicht inzichtelijk gemaakt.
Voor eventuele overlap in de toezichthoudende taken hebben beide partijen een samenwerkingsprotocol afgesloten.
Mochten de toezichthouders daartoe aanleiding zien dan kunnen zij handhavend optreden.

De leden van de fractie van **D66** wijzen erop dat in de memorie van toelichting voor toezicht en handhaving een verbinding wordt gelegd met het wetsvoorstel Wet Cliëntenrechten Zorg, terwijl dit wetsvoorstel uiteindelijk in drie afzonderlijke wetsvoorstellen is opgesplitst. Dit roept bij de leden van de fractie van D66 de vraag op hoe het toezicht en de handhaving voor het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens nu is geregeld.
Nu het wetsvoorstel Wet Cliëntenrechten Zorg in de oorspronkelijke vorm is komen te vervallen, krijgen de bepalingen van dit wetsvoorstel met betrekking tot de toestemmingseisen en informatieplicht bij elektronische gegevensuitwisseling, het recht op elektronische inzage en afschrift, de eisen die gelden voor de loggegevens en de verbodsbepalingen voor zorgverzekeraars, bedrijfsartsen, verzekeringsartsen en keuringsartsen een plaats in de Wet gebruik burgerservicenummer in de zorg. Vanwege de daarmee te wijzigen reikwijdte van die wet zal de citeertitel na

inwerkingtreding zijn gewijzigd in Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.
Zoals aangegeven in de paragraaf 1.6 van de memorie van toelichting geldt dat het toezicht en de handhaving van de bepalingen die worden opgenomen in de Wet gebruik burgerservicenummer in de zorg is geregeld in de Kwaliteitswet zorginstellingen (Kwzi) en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) als onderdeel van het leveren van verantwoorde zorg. Het toezicht op het bieden van verantwoorde zorg wordt op grond van die wetten uitgeoefend door de Inspectie voor de gezondheidszorg (IGZ). Op grond van artikel 8 Kwzi kan bij de handhaving gebruik worden gemaakt van aanwijzingen, bevelen en bestuursdwang. In het kader van de handhaving kan de IGZ op grond van artikel 7 Kwzi patiëntendossiers inzien. Dat kan ook op grond van artikel 87 Wet BIG voor zover het toezicht zich richt op een individuele zorgverlener. Verder is het op grond van de Wet BIG natuurlijk mogelijk om via het tuchtrecht op te treden tegen individuele zorgverleners die op onzorgvuldige wijze met patiëntgegevens omgaan.
Op grond van artikel 5 Kwzi, dient de zorgaanbieder jaarlijks verslag uit te brengen over het beleid dat hij heeft gevoerd in het kader van de kwaliteit van de zorg, waarbij de zorgaanbieder ook zal moeten ingaan op zijn beleid inzake het op veilige wijze verwerken van cliëntgegevens. Het niet voldoen aan deze verantwoordingsplicht door zorgaanbieders, kan worden bestraft met een bestuurlijke boete van maximaal € 33 550,–.
Voor het toezicht en de handhaving is ook het College Bescherming Persoonsgegevens (CBP) van belang, dat toeziet op de naleving van de Wbp. Het CBP is bij uitstek de instantie om erop toe te zien dat geen misbruik gemaakt wordt van de beschikbare informatie. De technische en organisatorische eisen voor elektronische uitwisselingssystemen worden opgenomen in een AMvB op grond van artikel 26 Wbp. Ten aanzien van de in deze AMvB gestelde regels is het CBP eveneens de toezichthouder. Op grond van artikel 61, vijfde lid, van de Wbp, kunnen verantwoordelijken voor de gegevensverwerking in het kader van het toezicht door het CBP, geen beroep doen op hun geheimhoudingsplicht. Ter handhaving van het bepaalde bij of krachtens de Wbp kan het CBP een last onder bestuursdwang of een dwangsom opleggen.
De door de fractie van D66 aangehaalde wetsvoorstellen waarin de Wet Cliëntenrechten Zorg is opgesplitst, spelen geen rol bij het toezicht en de handhaving van het voorliggende wetsvoorstel.

4 Reacties derden

Meerdere fracties (**VVD**, **SP**, **D66**) verzoeken een reactie op de vragen die een aantal brancheorganisaties heeft gesteld in hun aan uw Kamer gerichte brief van 13 februari 2015.

1. Verzoek om de eis van gespecificeerde toestemming niet in de wet vast te leggen dan wel de inwerkingtreding ervan voor onbepaalde tijd uit te stellen.
   De eis van gespecificeerde toestemming is nadrukkelijk op verzoek van de Tweede Kamer, amendement Bruins Slot (Kamerstukken 33 509, nr. 13), opgenomen in dit wetsvoorstel. Zonder deze eis, zijn we terug bij generieke toestemming en daar hebben de leden van de Tweede Kamer zich duidelijk negatief over uitgesproken.
   De doelstelling van gespecificeerde toestemming is om de cliënt bewuste keuzes te laten maken ten aanzien van het geven van toestemming. De specificatie houdt in dat de cliënt bij het geven van toestemming kan aangeven welke gegevens hij beschikbaar wil laten stellen – bepaalde gegevens of alle gegevens – en aan welke categorieën van zorgaanbieders of individuele zorgaanbieders hij die gegevens beschikbaar wil stellen. De cliënt geeft die gespecificeerde toestemming op basis van de informatie die hij daarover op grond van

artikel 15c dient te ontvangen. Die informatie zal het geven van uitdrukkelijke gespecificeerde toestemming goed moeten faciliteren. Dit wetsvoorstel schrijft niet een specifiek systeem voor. Gelet op artikel 15a, tweede lid, zal een systeem voor het registeren van de gespecificeerde toestemming minimaal het onderscheid naar categorieën van zorgaanbieders moeten kunnen maken. Indien een cliënt bezwaar maakt tegen dit aggregatieniveau, kan de cliënt besluiten een gehele categorie van zorgaanbieders geen toestemming te geven voor het *beschikbaar maken* van zijn of haar gegevens. Het omgekeerde is eveneens mogelijk: als de cliënt wel toestemming geeft zijn gegevens beschikbaar te stellen voor een bepaalde categorie zorgaanbieders, kan hij op het moment dat een zorgaanbieder uit die bepaalde categorie hem toestemming vraagt bij het aangaan van een nieuwe behandelrelatie zijn gegevens te *raadplegen*, die toestemming weigeren.
De bepaling is uiteraard niet bedoeld om een technisch onwerkbaar systeem op te tuigen. Zoals ook aangegeven in de brief van de brancheorganisaties zijn diverse veldpartijen momenteel gezamenlijk bezig te verkennen hoe gekomen kan worden tot een werkbare systematiek voor zowel zorgaanbieder als cliënt. Het benoemen van een exact moment waarop systemen technisch gereed zullen zijn, is momenteel nog niet haalbaar. Ik vind het echter van belang dat er spoedig een voorstel ligt van de veldpartijen over het traject naar een werkbare systematiek en binnen welke termijn dit gerealiseerd kan worden. Om niet vooruit te lopen op de feiten wordt pas na de behandeling van het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens in de Eerste Kamer een ingangsdatum voor inwerkingtreding van de wet bepaald, waarbij wordt uitgegaan van een realistische termijn.

2. Hoe moet de gespecificeerde toestemming worden gelezen in het kader van het uitsluiten van individuele zorgaanbieders.
Op grond van artikel 15a, eerste en tweede lid, zal een uitdrukkelijke gespecificeerde toestemming gelden bij het gebruik van een elektronisch uitwisselingssysteem. Er wordt geen systeem voorgeschreven, zodat – mits voldaan wordt aan de technische en organisatorische eisen – verschillende systemen denkbaar zijn. De gespecificeerde toestemming is bedoeld om een client bewust te laten bepalen waarvoor hij toestemming geeft en niet mag worden volstaan met generieke toestemming. Hij maakt die keuze op basis van de informatie over de inrichting van het systeem en hij moet ten minste kunnen kiezen voor bepaalde categorieën van zorgaanbieders. Daarbij is het zo dat een zorgaanbieder een individuele zorgverlener kan zijn die niet bij een zorginstelling werkt, maar vaker zal een zorgaanbieder een zorgaanbieder zijn als bedoeld in artikel 1 van de Kwaliteitswet zorginstellingen. Gespecificeerde toestemming strekt zich dus niet uit naar alle individuele zorgverleners. Daarvoor geldt dat binnen een specifieke behandelrelatie door de zorgverlener op grond van artikel 15b uitdrukkelijke toestemming moet zijn verkregen, alvorens hij gegevens die beschikbaar zijn in een elektronisch systeem mag gaan raadplegen.
3. Als een zorgaanbieder geen goede zorg kan waarborgen omdat hij geen toestemming krijgt van de patiënt gegevens in te zien of uit te wisselen moet hij indien nodig de behandelingsovereenkomst kunnen opzeggen.
De zorgaanbieder is – of hij zijn gegevens nu elektronisch uitwisselt of niet – altijd verantwoordelijk voor de juistheid en actualiteit van de inhoudelijke medische gegevens. De zorgaanbieder heeft een onderzoeksplicht en hij mag nooit volledig of uitsluitend vertrouwen op gegevens die al dan niet elektronisch zijn aangeleverd door andere zorgaanbieders. Dat geldt ongeacht de situatie waarin hij wel of niet is

uitgesloten van inzage in een systeem voor elektronische gegevensuitwisseling en ook ongeacht het feit of er veel of weinig gegevens zijn afgeschermd. Daarnaast moet de cliënt op grond van artikel 7:452 BW naar beste weten de inlichtingen en de medewerking geven die de hulpverlener redelijkerwijs voor de uitvoering van de behandelingsovereenkomst behoeft. Ook als de cliënt geen toestemming heeft gegeven voor elektronische gegevensuitwisseling. Zowel de zorgaanbieder als de cliënt hebben de vrijheid om wel of niet deel te nemen aan gegevensuitwisseling via een elektronisch uitwisselingssysteem. Uiteraard geldt dat als de zorgaanbieder over te weinig informatie kan beschikken voor een goede behandeling, hij de behandelrelatie kan opzeggen, dit is niet afhankelijk van de wijze waarop de zorgaanbieder zijn gegevens verzamelt c.q. of hij daarbij gebruik maakt (kan maken) van een elektronisch uitwisselingssysteem.

4. Kan de Minister bevestigen dat het toestemmingsvereiste niet geldt voor zorg verleend in het gedwongen of verplichte kader te weten de Wet zorg en dwang, de Wvggz en nu nog de huidige Wet Bopz.
Hierbij zij opgemerkt dat het gaat om de toestemming op grond van artikel 15b om gegevens te mogen raadplegen. Als de cliënt immers bij de opt-invraag op grond van artikel 15a voor de categorie van GGZ-zorgaanbieders geen gespecificeerde toestemming heeft gegeven, dan zijn er over deze cliënt geen gegevens raadpleegbaar. GGZ-zorgaanbieders die zijn aangesloten op een elektronisch uitwisselingssysteem zullen in principe gewoon op grond van artikel 15b aan de cliënt toestemming moeten vragen alvorens zij beschikbare gegevens kunnen raadplegen. Alleen in geval van het voorbereiden van een zorgmachtiging of een crisismaatregel, geldt een uitzondering bij het vragen van toestemming. Het gaat dan om situaties dat een cliënt zich verzet tegen zorg of opname terwijl die zorg wel noodzakelijk is ter voorkoming van schade of ernstig nadeel.

5. Als de bepaling in Artikel 15d, eerste lid impliceert dat een zorgaanbieder verplicht is een elektronisch dossier bij te houden betekent dat dat niet alle zeggenschapsrechten ten aanzien van een dergelijk dossier geëffectueerd kunnen worden. Het recht op elektronische inzage in en afschrift van een elektronisch dossier zou beter in de Wgbo opgenomen kunnen worden aangezien het onderhavige wetsvoorstel vooral betrekking heeft op het gebruik van elektronische uitwisselingssystemen door zorgaanbieders en niet zozeer gaat over interne cliëntdossiers.
Met dit wetsvoorstel wordt geen nieuw doel voor het medisch dossier vastgelegd en daarmee wordt de WGBO ongemoeid gelaten. Een zorgaanbieder legt een dossier aan dat hij nodig heeft voor goede en verantwoorde zorgverlening. Dit kan elektronisch, maar dat is niet verplicht. Ook nu al heeft een cliënt op grond van de Wgbo recht op inzage in en afschrift van het hem betreffende dossier. Daaraan wordt in dit wetsvoorstel het recht op elektronische inzage en afschrift toegevoegd. De inhoud of vorm van een dossier zal daarvoor niet hoeven te veranderen. Op grond van artikel 15d, eerste lid, Wbns-z, kan een cliënt zijn zorgaanbieder ook verzoeken van een papieren dossier een elektronisch afschrift te verschaffen.
Het wetsvoorstel introduceert een aantal normen dat specifiek betrekking heeft op *elektronische* verwerking van gegevens in de zorg. De in dit wetsvoorstel opgenomen bepalingen zien toe op deze specifieke vorm van verwerking van gegevens in de zorg en zijn om die reden bij elkaar in een apart wetsvoorstel geplaatst.

6. Waarom voldoen de bestaande sanctiemogelijkheden niet bij onrechtmatige raadplegingen?
De toevoeging van artikel 15 i is wenselijk omdat misbruik van patiëntengegevens moet worden gezien als een ernstig vergrijp. Niet alleen wordt hiermee de privacy van een persoon geschaad en kan

hieruit voor de desbetreffende persoon schade voortvloeien, ook het vertrouwen in elektronische gegevensuitwisseling als middel om efficiënt en betrouwbaar gegevens uit te wisselen tussen zorgaanbieders kan in ernstige mate geschaad worden.

Op zorgverleners rust een bijzondere plicht om geen misbruik van elektronische uitwisse-lingssystemen te maken. Daarom is het gewenst dat als extra sanctie wordt voorzien in de bijkomende straf van ontzetting van het recht het beroep uit te oefenen waarin de feiten zijn begaan.

Daarbij is mede een overweging dat het tuchtrecht geen mogelijkheden biedt om beroepsbeoefenaren die niet geregistreerd zijn ingevolge artikel 3 van de Wet BIG, maar die ingevolge artikel 34 van de Wet BIG wel een beschermde titel hebben, tuchtrechtelijk ter verantwoording te roepen. Zij vallen immers niet onder de reikwijdte van het tuchtrecht. Dat is alleen van toepassing op beroepsbeoefenaren die ingevolge artikel 3 van de Wet BIG in het BIG-register geregistreerd zijn. Zij kunnen door de tuchtrechter dan ook niet uit hun beroep worden ontzet. Door het mogelijk te maken dat ook de strafrechter een beroepsbeoefenaar bij misbruik van patiëntengegevens door computervredebreuk of schending van de geheimhoudingsplicht, uit zijn beroep kan ontzetten, kunnen ook deze beroepsbeoefenaren voldoende streng worden bestraft.

7. Hoe kan een hulpverlener voorkomen dat een ouder zich online toegang verschaft tot het medisch dossier van het kind wanneer tegen deze ouder een vermoeden van kindermishandeling bestaat.
8. Hoe kan voorkomen worden dat informatie over (een vermoeden van) kindermishandeling verwijderd wordt.

   Ouders die niet uit de ouderlijke macht zijn ontzet hebben ook nu al het recht om het medisch dossier van hun kind in te zien. Of de toevoeging van het recht op elektronische inzage een negatief effect zal hebben op de bestrijding van kindermishandeling valt dan ook moeilijk in te zien. Wel moet worden opgemerkt dat de laatste volzin van artikel 7:457, derde lid BW (indien de hulpverlener door inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege) ook bij elektronische inzage onverkort van toepassing blijft. Dit betekent dat bij een vermoeden van kindermishandeling door de arts kan worden besloten het recht op inzage in het dossier van het kind aan de ouders te weigeren of niet te voldoen aan de wens van ouders om gegevens te vernietigen. Dit punt moet goed overwogen worden bij het opzetten van systemen waarbij cliënten op elk gewenst moment kunnen inloggen om hun dossier of dat van hun kind in te zien. Hoe het recht op inzage in gevallen als voormeld in de praktijk zal worden beperkt is dan ook aan het veld.
9. Wat verstaat de Minister onder een (kosteloos) elektronisch afschrift en hoe wordt het financieringsmodel hierop aangepast.

   Met het wetsvoorstel geef ik geen nadere invulling aan de vorm van het afschrift. Dat is aan de zorgaanbieder zelf. Voor een papieren afschrift kan inderdaad een redelijke vergoeding worden gevraagd op grond van artikel 7:456 BW, omdat het afdrukken op papier kosten met zich meebrengt waarvan het niet redelijk is dat die voor rekening van de zorgaanbieder zouden zijn. Daarvan is bij een elektronisch afschrift geen sprake, aanpassing van het financieringsmodel is dan ook niet aan de orde.
10. Wordt het financieringsmodel aangepast op de verplichting cliënten te informeren over hun rechten bij elektronische gegevensuitwisseling.

   Het actief en juist informeren is een onderdeel van het geven van verantwoorde zorg. Zorgaanbieders hebben op grond van artikel 34, eerste lid, van de Wbp de plicht om duidelijke voorlichting te geven over het doel en de reikwijdte van het verkrijgen en verwerken van

gegevens, ook als die afkomstig zijn via een elektronisch uitwisselingssysteem. Het financieringsmodel zal en hoeft hierop niet te worden aangepast.

11. Moet er een aparte registratie worden bijgehouden van verleende toestemmingen.
Met dit wetsvoorstel worden zorgaanbieders inderdaad verplicht om de door de cliënt verleende toestemming te registeren evenals het moment waarop de toestemming van kracht is geworden.
Of die gegeven toestemming alleen in het systeem van de zorgaanbieder zichtbaar is of ook zichtbaar is via het elektronisch uitwisselingssysteem, zal afhangen van de technische vormgeving en wordt niet voorgeschreven. Een systeem waarin dat voor alle gebruikers zichtbaar is, is natuurlijk wel het meest transparant. Het is aan de zorgaanbieder deze afweging te maken.
12. Zijn behalve zorgverzekeraars, bedrijfsartsen en verzekeringsartsen ook andere financiers van medisch-specialistische zorg zoals gemeenten en het Ministerie van Veiligheid en Justitie en daaraan verbonden zorgaanbieders uitgesloten van toegang tot elektronische uitwisselingssystemen.
Het wetsvoorstel legt aan zorgverzekeraars een verbod op om zich toegang te verschaffen tot elektronische uitwisselingssystemen. Voor zover een zorgaanbieder werkzaamheden verricht als bedrijfsarts, verzekeringsarts, dan wel als keurend arts voor keuringen als bedoeld in de Wet op de medische keuringen, mag hij zich op grond van artikel 15f, tweede lid van het wetsvoorstel geen toegang verschaffen tot elektronische uitwisselingssystemen en gegevens uit elektronische uitwisselingssystemen verwerken. Verder is het zo dat alleen *zorgaanbieders* toegang kunnen krijgen tot een elektronisch uitwisselingssysteem. Medewerkers van een gemeente of ministerie treden niet op als zorgaanbieder, voor hen is toegang tot een elektronisch uitwisselingssysteem in het geheel niet aan de orde. Hetzelfde geldt voor degenen die als financier optreden.
Het wetsvoorstel hoeft hiervoor derhalve niet te worden aangepast.
13. Mogen bedrijfsartsen, verzekeringsartsen of andere keurende artsen ook onderling geen cliëntgegevens uitwisselen via een elektronisch uitwisselingssysteem.
Dat hangt af van het doel waarmee de bedrijfsarts, verzekeringsarts of andere keurende arts onderling informatie uitwisselen.
In artikel 15 f van het wetsvoorstel staat in lid 2 opgenomen dat voor zover een zorgaanbieder werkzaamheden verricht als bedrijfsarts, verzekeringsarts, dan wel als keurend arts voor *keuringen* als bedoeld in de Wet op de medische keuringen, hij zich geen toegang verschaft tot elektronische uitwisselingssystemen en geen gegevens verwerkt uit elektronische uitwisselingssystemen. Dat betekent dat hij als arts wel mag zijn aangesloten op een elektronisch uitwisselingsysteem en dat hij bij het verlenen van zorg, na het vragen van toestemming of hij gegevens van de cliënt mag raadplegen, beschikbare en relevante gegevens mag inzien.
De werkzaamheden die reïntegratiedeskundigen, arbeidsdeskundigen, jobcoaches en werkcoaches verrichten, vallen niet onder het begrip zorg en dus niet onder de werking van deze wet.
Voor zover de bedrijfsarts, keurings- en verzekeringsarts geen zorg verlenen is de Wbp onverkort van toepassing.
14. De KNMG c.s. stelt dat de zorginformatiesystemen van zorgaanbieders moeten worden aangepast om te voorkomen dat administratief medewerkers toegang hebben tot het volledige dossier. Men vraagt hoeveel tijd de praktijk hiervoor krijgt en of het financieringsmodel hierop wordt aangepast.
Ook onder de huidige wet- en regelgeving is de zorgaanbieder verantwoordelijk voor het treffen van maatregelen om te voorkomen

dat medewerkers die geen volledige toegang mogen hebben tot een dossier, die toegang ook daadwerkelijk niet hebben. Ter toelichting het volgende. In het licht van de Wbp kan de zorgaanbieder als verantwoordelijke van persoonsgegevens, deze gegevens laten verwerken door een bewerker, bijvoorbeeld een administratief medewerker. De zorgaanbieder moet ervoor zorgen dat er voldoende waarborgen aanwezig zijn ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De zorgaanbieder moet toezien op de naleving van die maatregelen.
In die zin verschilt de huidige situatie niet met de situatie na inwerkingtreding van het wetsvoorstel.

15. Wie is verantwoordelijk voor het niet beschikbaar stellen of raadplegen van gegevens die wel beschikbaar hadden moeten zijn c.q. geraadpleegd hadden moeten worden.
Voor het antwoord hierop wordt verwezen naar het antwoord op de vraag naar het mogen beëindigen van de behandelrelatie (vraag 3). In dat antwoord is de verantwoordelijkheidsverdeling tussen cliënt en zorgaanbieder uiteengezet.
16. In hoeverre is in het wetsvoorstel afgedekt dat niet alle zorgverleners alle informatie te zien krijgen.

Het wetsvoorstel regelt dat cliënten gespecificeerde toestemming geven. Gespecificeerde toestemming betekent dat de cliënt toestemming geeft voor het elektronisch ter beschikking stellen van alle of bepaalde gegevens aan bepaalde aan te duiden zorgaanbieders of categorieën van zorgaanbieders waarmee deze cliënt een behandelrelatie heeft of krijgt en die zijn aangesloten op dat elektronisch uitwisselingssysteem. Alle zorgaanbieders die de cliënt niet heeft benoemd zijn automatisch uitgesloten om zijn gegevens te raadplegen. Voor alle toestemming tot raadpleging geldt dat die toestemming zich alleen uitstrekt tot het raadplegen van gegevens die noodzakelijk zijn voor een goede uitvoering van de behandelrelatie. Toestemming voor raadpleging is, net als nu het geval is met papieren dossiers, geen vrijbrief voor het rondneuzen in alle beschikbare gegevens van een cliënt. Het is aan de beheerders en zorgaanbieders om hier technisch invulling aan te geven en gedragscodes op te stellen.

Meerdere fracties (**SP**, **D66**) vragen een reactie op de brief van VP Huisartsen d.d. 16 februari 2015. Deze belangenvereniging vraagt zich af of met dit wetsvoorstel de in de WGBO vastgelegde veronderstelde toestemming bij gegevensoverdracht naar een direct bij de behandeling betrokken zorgverlener overeind blijft.
Huisartsen onderhouden met hun cliënten een permanente behandelrelatie. Op grond van artikel 15b dient eenmalig aan de cliënt toestemming te worden gevraagd om gegevens die beschikbaar worden gesteld via een elektronisch uitwisselingssysteem te mogen raadplegen. Die toestemming geldt dan ook voor zijn waarnemer of anderen die bij de behandelrelatie zijn betrokken. Indien ziekenhuizen en huisartsen gaan werken met pull-verkeer voor het ophalen van labuitslagen en specialistenbrieven, zal daarvoor op grond van de opt-in uitdrukkelijke toestemming moeten worden gegeven. Dit is mijns inziens echter alleen maar zo als die labuitslagen en brieven daarmee voor alle op het elektronisch uitwisselingssysteem aangesloten zorgaanbieders beschikbaar worden. Indien er sprake is van een portal waarmee door middel van bijvoorbeeld een inlogcode alleen de eigen huisarts die gegevens kan ophalen, dan is er feitelijk een zelfde situatie als bij push-verkeer en mag worden uitgegaan van veronderstelde toestemming op grond van de WGBO.

De leden van de fractie van **D66** vragen een reactie op de brief van Privacy First d.d. 20 februari 2015.
In de brief van Privacy First staat dat gespecificeerde toestemming tot het probleem leidt dat op basis van toestemming bij één zorgverlener het dossier van meerdere zorgverleners kunnen worden ontsloten en dat deze gespecificeerde opt-in niet voldoet aan de eis van expliciete en geïnformeerde toestemming van artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM) en aan de WGBO.
Op grond van artikel 15a, eerste en tweede lid, van het voorstel, kan een zorgaanbieder slechts gegevens beschikbaar stellen via een elektronisch uitwisselingssysteem indien de cliënt daarvoor uitdrukkelijke en gespecificeerde toestemming heeft gegeven. De specificatie houdt in dat de cliënt bij het geven van toestemming moet aangeven welke gegevens hij beschikbaar wil laten stellen – bepaalde gegevens of alle gegevens – en aan welke categorieën van zorgaanbieders of individuele zorgaanbieders hij die gegevens beschikbaar wil stellen. De cliënt geeft die gespecificeerde toestemming op basis van de informatie die hij daarover op grond van artikel 15c dient te ontvangen. Die informatie zal het geven van uitdrukkelijke gespecificeerde toestemming goed moeten faciliteren. Het zal bijvoorbeeld niet voldoende zijn om aan te geven dat alle fysiotherapeuten in de regio zijn aangesloten als niet duidelijk is tot waar de regio zich uitstrekt. Om als cliënt gespecificeerde toestemming te kunnen geven, moet helder zijn welke zorgaanbieders horen bij een aan te duiden categorie. Alle medisch specialisten in Utrecht als categorie is niet gespecificeerd genoeg, de medisch specialisten van ziekenhuis X of de internisten van ziekenhuis Y en Z wel.
Op grond van het oorspronkelijke artikel 15a, tweede lid, was het mogelijk dat een cliënt generieke toestemming zou geven voor het beschikbaar stellen van gegevens aan alle op een bepaald elektronisch uitwisselingssysteem aangesloten zorgaanbieders. Het zou dan mogelijk zijn geweest dat via de registratie van die generieke toestemming in het elektronisch uitwisselingssysteem voor andere zorgverleners die een behandelrelatie hebben met die cliënt, duidelijk zou zijn dat ook zij toestemming hadden om gegevens beschikbaar te stellen. Nu artikel 15a, tweede lid, zodanig is ingekaderd dat een cliënt zijn toestemming altijd moet specificeren, is die mogelijkheid een stuk beperkter. Maar het is wel denkbaar dat apotheek X in plaats Y tegelijk voor alle apotheken in plaats Y toestemming vraagt om de medicatiegegevens beschikbaar te stellen. Er is in zo'n geval voldaan aan het vereiste van expliciete en geïnformeerde toestemming.
Omdat het geven van generieke toestemming niet is toegestaan, is de veronderstelling van Privacy First dat met eenmalige toestemming bij één zorgverlener de medische gegevens van alle ander zorgverleners waarmee de cliënt contact heeft, kunnen worden ontsloten, daarom onjuist.
Privacy First stelt ook dat er bij uitbreiding van het systeem wordt uitgegaan van impliciete toestemming, waardoor er feitelijk sprake is van een opt-out model. Gelet op het feit dat de toestemming altijd gespecificeerd moet zijn, geldt het volgende. Als een cliënt gespecificeerde toestemming heeft gegeven aan zijn huisarts om zijn gegevens beschikbaar te stellen aan bijvoorbeeld de categorie fysiotherapeuten in de regio Zaanstreek, dan hoeft die cliënt op grond van artikel 15c, eerste lid niet te worden geïnformeerd over de aansluiting van een nieuwe fysiotherapiepraktijk in die regio. Een substantiële uitbreiding van het systeem waarover de cliënt geïnformeerd moet worden is wel de uitbreiding van de regio. De cliënt heeft immers gespecificeerde toestemming gegeven voor de fysiotherapeuten in de regio Zaanstreek en niet voor de regio West-Friesland. Gelet op het vereiste van uitdrukkelijke gespecificeerde toestemming, kan het aanpassen van de toestemming als bedoeld in artikel 15c, eerste lid, nooit een opt-outregeling zijn. Bij een

uitbreiding van het systeem moet uitdrukkelijke gespecificeerde toestemming zijn gegeven. Alleen vanaf dat moment kan die uitbreiding op de toestemming van een bepaalde cliënt van toepassing zijn.

De Minister van Volksgezondheid, Welzijn en Sport,
E.I. Schippers